Why do we need new recommandations on profiling...

Poullet, Yves

Publication date:
2020

Document Version
Publisher's PDF, also known as Version of record

WHY DO WE NEED NEW RECOMMANDATIONS ON PROFILING…

Webinar Council of Europe 01/07/20

©Yves Poullet – Emeritus Professor at the University of NAMUR and UCLille – Cochairman of NADI

Ten years ago, the Council of Europe has adopted a Recommendation on Profiling. That Recommendation was welcomed as an answer to the development of profiling activities in different sectors, especially for marketing purposes. Today, profiling is everywhere. As regards marketing, profiling is used not only for detecting adequate advertisements according to the consumers characteristics but also for selecting them or adapting the prices. Profiling is broadly used within the medical sector, especially as regards the use of genetic data. Employers make recourse to profiling for selecting their employees or evaluating them. Administrations are using profiling for defining strategies and for applying the public regulations including for detecting fiscal or social security fraudsters or calculating sanctions for criminals. Facial recognition is becoming more and more a common tool for Law Enforcement Authorities' investigations. Politicians are using profiling techniques in order to have a better knowledge of their supporters or for adapting their speeches in order to maximize their chances to be elected. In all public and private sectors, profiling definitively is the adequate way for optimizing and securing their activities.

That extension is due in great part by the generalization of the use of machine learning systems more and more powerful and connected with big data. These big data are collecting infinite number of data, trivial or not, anonymous, pseudonymised or not, from sources more and more numerous. They are operating that collection through sensors and terminals of all types within an interconnected world. In the extended report we have produced last year for the Consultative Committee about Convention n°108, we have distinguished different machine learning systems, supervised or not, simple or deep learning, what we usually call "Artificial Intelligence" techniques. It is quite clear that nobody will deny the benefits of these new techniques but in the same time we must be aware of the risks linked by these technologies which ten years after the writing of the first recommendations obliges to enlarge the scope and to deepen certain considerations,

We need new recommendations to face that extension and these new techniques of profiling because Artificial intelligence has substantially modified the functioning, the actors and the risks of Profiling The first point is the fact that **modern profiling is no more necessarily linked with profiles, defined as a set *of data characterising a category of individuals that is intended to be applied to an individual. I*n machine learning, many "models" do not explicitly manipulate profiles but are directly applied to the data collected and make decisions or predictions without any 'profile' interface. Furthermore,** modern profiling is based on statistical aggregation of vast amount of data and no more on logic causation, which definitively permits to ensure a transparent functioning. Modern profiling is often functioning apart from complex and unpredictable interactions of neural networks. Even if certain procedures of supervision, auditability or explainability might be used, the algorithms functioning remains more or less opaque. That opacity creates major risks since bias (for instance data not updated, partial or irrelevant) and error programming are consciously or unconsciously possible.

Beyond that, our report pinpoints the number of actors involved in the functioning of these systems, whose liability has to be defined according to their participation. Certain obligations like the obligation to give the main parameters of the data bases or the code source of the algorithms might be imposed. As regards actors, a special attention must be reserved to the role of the Information and communication platforms. As gatekeepers of the information society, they are ideally placed to collect data and establish profiles for themselves and their numerous subsidiaries or customers data

Finally, modern profiling amplifies the risks faced by individuals: risk of reductionism, risks of normalization) and due, in particular, to its predictive capacities, the risks of stigmatization and of manipulation. Beyond these risks covered by traditional data protection legislation, modern profiling creates collective risks at different levels which are not taken or only taken partly into consideration by data protection legislation. Cambridge Analytica is an example of the fact that profiling might be used as a way to challenge our democracies. One to one insurance is another example how the principle of 'pooling', which at least was a key principle of the insurance sector, is called into question by the AI. Last point but I consider as the main point, big data analyses is no longer gathered about one specific individual or small group of people but rather about large and undefined groups and leads to define new categories of people totally unpredictable. If under the conclusions of an AI system, I say 'the chess players

of more than 50 years, single and having a red car are 90 procent potential criminals", you imagine the consequences for myself but also for people around the world unknown from myself who are chess players and… To be short: the problem shifts from individual's protection to 'groups' protection, taking into account the question of social justice and discrimination. This type of finding poses a difficulty under data protection law, which is only concerned with the protection of individuals and leaves groups' protection issues in the shadows. Furthermore, discrimination aspects are analyzed from the DP laws only through the special categories of data and are unable to face the unpredictable grouping deduced from AI systems.

Second major reason to adopt new recommendations. Since 2010, different legal provisions and documents have been enacted. These documents, to the extent that they apply or are aimed at profiling activities, deserve to be taken into account**. I just pinpoint three documents from the Council of Europe itself. The revision of the Convention 108 contains no expli**cit reference to profiling but art. 9.1. a) on automated decision making and art. 10. 1 and 2 and the accountability principle and importance of the risk approach are source of inspiration. More important are the two guidelines issued by the Consultative Committee one on Big data, the second one on Artificial intelligence. I quote a passage highlighting the need to move beyond a purely individualistic approach as regards the risks associated with emerging technologies: « *Since the use of Big Data may affect not only individual privacy and data protection, but also the collective dimension of these rights, preventive policies and risk-assessment shall consider the legal, social and ethical impacts of the use of Big Data, including with regard to the right to equal treatment and to non-discrimination*." And I underline also the provisions about the new obligations imposed to each participants building up the profiling systems.

It is quite interesting to see that EU GDPR has taken again the C of E recommendation's definition of the profiling and certain provisions about the duty to inform about the "logic behind an automated decision" and the right to obtain explanation about the criteria taken into account in an automated decision. We also underline that certain 'high risk' profiling systems have to be, under article 35 GDPR, be evaluated through a PIA procedure.

More important, these three last years, a lot of recommendations and regulatory texts of different nature have been produced about the ethical questions and principles which have to govern AI activities. Among them, I would like to get

your attention to EU Parliament Resolution containing recommendations to the Commission on framework of ethical aspects of artificial intelligence, robotics and related technologies dated from the 21st of April. The Resolution and the Regulation proposed require that ethical values (dignity, social justice and not only autonomy) are taken into consideration. Particularly, as regards "high risk" AI systems, the evaluation has to be achieved by an independent board after a multidisciplinary and multistakeholders discussion. Member states are invited to set up Data Ethics Committees in order to evaluate and eventually to label Big data or AI systems.

In that technological and regulatory context, we are of opinion that it is time to propose certain modifications to the present recommendations on profiling. We have selected some provisions around three major themes: 1.enlargement of the scope of the recommendations; 2. Need for a multidisciplinary and multistakehoders risk assessment 3. Reinforcement of the DS Rights

As regards the **enlargement of the scope**, I quote the main provisions thereabout:

'The respect for fundamental rights and freedoms, notably the right to privacy and the principle of non-discrimination, but also the imperatives of social justice, cultural diversity and democracy, shall be guaranteed during the processing of personal data subject to this recommendation. Profiling must contribute both to the well-being of individuals and to the development of an inclusive, democratic and sustainable society.' (2.1)

This enlargement has, at our point of view, two consequences: the first one leads to impose to DP supervisory authorities to cooperate with consumer and competition protection authorities as well as with institutions responsible for equal opportunities or for the promotion of democracy; the second one is an extension of supervisory authorities' competence to the analysis of collective risks and risks to the society and its democratic functioning and to ensure the respect of principle 2.1.

As regards **the need for an *'a priori'* evaluation of the risks, the new text provides a specific recommendation of a continuous risk assessment about profiling systems based on machine learning, especially when it concerns high-risk profiling systems and especially as regards deep learning systems. This assessment must be multidisciplinary and multistakeholders and led by competent professionals.**

Furthermore, “Member states and supervisory authorities should encourage the setting up of independent and qualified certification mechanisms for AI and data protection systems and related labels and marks to demonstrate that processing operations carried out by controllers and processors comply with this recommendation.”

The recommendation envisages also the problem of the multiplication of sensors used for collecting data: “*The distribution and use, without the data subject’s knowledge, of software aimed at the observation or the monitoring in the context of profiling of the use being made of a given terminal or electronic communication network should be permitted only if they are expressly provided for by domestic law and accompanied by appropriate safeguards*”.

Third and last theme: **Reinforcement of the DS Rights. A lot of new provisions are proposed on that point.**

So, the autonomy of the DS has to be reinforced. On that question, we quote:

- Profiling should not be carried out for the purpose of manipulating data subjects (2.4).
- The possibility of opting out as regards the profiling and the choice between the different profiling purposes or degrees. It is quite clear that the use of profiled services (for instance as regards the offering music listening services)
- In order to ensure free, specific and informed consent to profiling, providers of information society services should ensure, by default, non-profiled access to information about their services
- Unless explicitly consented to, the data subject must be able to object by an easy means to the transfer or sharing of data, either for profiling purposes by third parties or of the results of profiling

Besides these principles, we provide a data controller’s obligation to inform (by icon) about its use of profiling systems and their main characteristics and about the major problem of decision based on an automated system, we recommend that:

- the controller considers all the particularities of the data and not only rely on decontextualized information or results of the processing;

- in the event of high-risk processing, the controller **sets up a service** where a person, *a human person having the competence to reanalyse the decision proposed or taken by the profiling system*, will inform the data subject of the algorithmic operations underlying the data processing, including the consequences of these operations for him/her. In that case, **the information should be such as to enable the data subject to understand the justification for the decisions or proposals for decisions regarding him/her**.
- where there are indications of direct or indirect discrimination based on the functioning of the profiling operation, controllers and processors shall provide evidence of the absence of discrimination.
- Persons affected by a decision based on profiling have the right to receive useful explanation of the decision and to challenge it in front of a competent authority having access to all the information about the profiling and its functioning.

It is time to conclude: We need trust in our more and more profiling society.

Regulation must be proportionate: Profiling means a lot of operations with different purposes and each of them must be regulated specifically according to the risks linked with each kind of profiling. Profiling activities might join together different actors , liable according with the role and the contribution of each of them

We need an interdisciplinary and continuous approach as regards the risks linked to a profiling activity taking into account not only DP concerns in the strict sense but also the collective and societal impacts

We must considerably reinforce the DS rights and education

An **interdiciplinary approach human centered** (Human 'in the loop', 'on the loop' and associated to the operation) must be developed internally but will find an adequate complement in the existence of an independent organism in charge of the continuous control of the quality at the largest sense, that means no bias, security and appropriateness of the algorithms.